said identity software being for use on said computer to [, with no effective protection against unauthorised use,] provide [an] identity information of said [the rightful or authorised] user [of said authorising software] ;

said identity information being for to be authenticated by a remote computing means [computer] in order for enabling [said remote computer to perform] operation(s) for which said [rightful or authorised] user has to be responsible, to be performed ; and the [presence] existence of said identity software in a memory under control of [on] said computer is being determined without a said operation being performed [by said remote computer] .

[ wherein use of said other software on said computer will be authorised if said] [identity software is determined as being present on said computer ; and said] [authorising software and said identity software being software meeting said existing] [standard .]

[ wherein said computer comprises no hardware specific to said rightful or] [authorised user for directly or indirectly authorising use of said protected software] [thereon.]

2.(Third time amended) Method [Authorising software, stored in a device or] [physically on a medium,] as claimed in claim 1, wherein further comprising steps of [software, when being executed, for] determining data integrity of said identity software ; and if the data integrity determination result is unfavourable, said identity software will further be determined as not [present] existing in a memory means under control of said computer .

3.(Third time amended) Method [Authorising software, stored in a device or] [physically on a medium,] as claimed in claim 1, wherein further comprising the steps of [authenticating software for, when being executed,] authenticating said computer as being a predetermined computer [; said authenticating software]

[comprises a stored information of configuration of said computer and software for,] [when being executed, determining configuration of said computer and for] [comparing the determined result with said stored information ;] , and if the [comparison] authentication result is unfavourable, said authorising software will not authorise use of said [other] protected software on said computer and will authorise use of said protected software on said computer if said authentication result is favourable and said identity software is determined as existing in a memory under control of said computer.

4.(Third time amended) Authorising software, stored in a device or existing physically on a medium, as claimed in claim 3, wherein said configuration of said computer includes the hardware configuration thereof.

5.(Third time amended) Authorising software, stored in a device or existing physically on a medium, as claimed in claim 3, wherein said configuration of said computer includes the software configuration thereof.

12.(Third time amended) [Software] Protection software , stored in a device or existing physically on a medium and being computer software conforming to or compatible with an existing standard, for use on a computer [which being made to meet] , to protect purchased commercial computer software by discouraging the rightful or authorised user thereof from enabling or allowing other person(s) to use said protected software or a duplication copy thereof ;

said computer conforming to or being compatible with said [an] existing standard [such] so that any software [product(s) meeting] conforming to or compatible with said standard can be used thereon and without modification thereof ;

said protection software comprising :

identity software for use on said computer to [, with no individual and] [effective protection , provided by execution of said software, against unauthorised] [use,] provide [an] identity information of [the rightful or authorised] said user [of an authorising software] , said identity information being for to be authenticated by a remote computing means [computer] in order for enabling [said remote computer to perform] operation(s) for which said [rightful or authorised] user has to be responsible, to be performed ;

authorising software for, when executed, authorising use of [other] said protected software [which being purchased, and being protected from unauthorised] [use,] on said computer ;

Wherein [said identity software and] said authorising software [are] is contained in said protection software in such a manner that said authorising software is prevented from being copied therefrom individually. [ ; and said authorising software and said identity software being software meeting said existing standard.]

[ wherein said computer comprises no hardware specific to said rightful or] [authorised user for directly or indirectly authorising use of said protected software] [thereon.]

13.(Third time amended) [Software] Protection software , stored in a device or existing physically on a medium, as claimed in claim 12, wherein said protected software comprises a plurality of protected programs; each of said [other software comprises] protected programs includes [an] validity information [stored at] in a first predetermined location therein for indicating a valid identity of its rightful user exists [at] in a second predetermined location therein , and an encrypted identity of its rightful user [at a respective location therein] ; and each of said [other software] protected programs, when being executed, will fail to operate if said validity information therein being altered or said identity therein and the decryption result of said encrypted identity therein being inconsistent.

15.(Third time amended) [Software] Protection software , stored in a device or existing physically on a medium, as claimed in claim 13, wherein further comprising an encrypted identity of its rightful user ; and if one of said [other software] protected programs stored in said computer has a valid user identity which being not consistent with the decryption result of said encrypted identity in said protection software , said authorising software will not authorise use of said [other software] protected programs.

16.(Third time amended) [Software] Protection software , stored in a device or existing physically on a medium, as claimed in claim 12, wherein said authorising software [comprises] includes said identity software.

17.(Third time amended) Authorising [software] program , stored in a device or existing physically on a medium and [meeting] conforming to or compatible with an existing standard, for use on a computer [which being made to meet], to protect commercial computer software by discouraging a user thereof from enabling or allowing other person(s) to use said protected software or a duplication copy thereof ;

said computer conforming to or being compatible with said existing standard [such] so that any software [product(s) meeting] conforming to or compatible with said standard can be used thereon and without modification thereof ;

said authorising [software] program being for, when [being] executed, [authorise other] authorising use of said protected software [which being protected] [ from unauthorised use, to be used] on said computer ;

wherein information representative of an [a same] encryption algorithm used by a means for providing [an] identity information of [the rightful or authorised] said user [of said authorising software], exists in said authorising [software] program and being accessible or, when said authorising [software] program being executed, usable by [a] the user thereof ;

said identity information being for to be authenticated by a remote computing means [computer] in order for enabling [said remote computer to perform] operation(s) for which said [rightful or authorised] user has to be responsible, to be performed .

[wherein said computer comprises no hardware specific to said rightful or] [authorised user for directly or indirectly authorising use of said other software] [thereon.]

19.(Third time amended) [Authorising] program software, stored in a device or existing physically on a medium, as claimed in claim 17, wherein said [other] protected software comprises a plurality of protected programs; each of said [other software comprises] protected programs includes [an] validity information [stored at] in a first predetermined location therein for indicating a valid identity of its rightful user exists [at] in a second predetermined location therein , and an encrypted identity of its rightful user [at a respective location therein] ; and each of said [other software] protected programs , when being executed, will fail to operate if said validity information therein being altered or said identity therein and the decryption result of said encrypted identity therein being inconsistent.

21.(Third time amended) Authorising [software] program , stored in a device or existing physically on a medium, as claimed in claim 19, wherein further comprising an encrypted identity of its rightful user ; and if one of said [other software] protected programs stored in said computer has a valid user identity not consistent with the decryption result of said encrypted identity in said authorising [software] program , said authorising [software] program will not authorise use of said [other software] protected programs.